ViPNet PKI Client File Unit Linux

Руководство пользователя

infotecs

ФРКЕ.00175-01 34 06

Версия продукта 1.5.0

АО «ИнфоТеКС»

127083, Москва, улица Мишина, д. 56, стр. 2, этаж 2, помещение IX, комната 29

Телефон: +7 (495) 737-6192, 8-800-250-0260 — бесплатный звонок из России (кроме Москвы)

Веб-сайт: infotecs.ru

Служба поддержки: hotline@infotecs.ru

Содержание

Введение

О документе

В данном документе рассматривается назначение и применение программы File Unit, которая входит в состав программного комплекса ViPNet PKI Client Linux (далее — ViPNet PKI Client). В руководстве описаны основные возможности программы, приведено описание пользовательского интерфейса.

Для кого предназначен документ

Данный документ предназначен для пользователей ViPNet PKI Client, которые собираются обеспечивать безопасность документов, передаваемых по открытым каналам связи или с использованием съемных носителей.

Соглашения документа

Ниже перечислены соглашения, принятые в этом документе для выделения информации.

Таблица 1. Обозначения, используемые в примечаниях

Обозначение	Описание
	**Внимание!** Указывает на обязательное для исполнения или следования действие или информацию.
	**Примечание.** Указывает на необязательное, но желательное для исполнения или следования действие или информацию.
	**Совет.** Содержит дополнительную информацию общего характера.

Таблица 2. Обозначения, используемые для выделения информации в тексте

Обозначение	Описание
Название	Название элемента интерфейса. Например, заголовок окна, название поля, кнопки или клавиши.
Клавиша+Клавиша	Сочетание клавиш. Чтобы использовать сочетание клавиш, следует нажать первую клавишу и, не отпуская ее, нажать вторую клавишу.
Меню > Подменю > Команда	Иерархическая последовательность элементов. Например, пункты меню или разделы на панели навигации.
`Код`	Имя файла, путь, фрагмент текстового файла (кода) или команда, выполняемая из командной строки.

При описании команд в данном документе используются следующие условные обозначения:

- Команды, которые могут быть выполнены только в режиме администратора, выделены красным цветом. Например:

  ```
  команда
  ```

- Параметры, которые должны быть заданы пользователем, заключены в угловые скобки. Например:

  ```
  команда <параметр>
  ```

- Необязательные параметры или ключевые слова заключены в квадратные скобки. Например:

  ```
  команда <обязательный параметр> [необязательный параметр]
  ```

- Если при вводе команды можно указать один из нескольких параметров, допустимые варианты заключены в фигурные скобки и разделены вертикальной чертой. Например:

  ```
  команда {вариант-1 | вариант-2}
  ```

О программе

Программа File Unit входит в состав ViPNet PKI Client и позволяет обеспечить безопасность передаваемых файлов с помощью шифрования (см. глоссарий, стр. 52) и электронной подписи (см. глоссарий, стр. 54).

Системные требования

Требования к компьютеру для установки ViPNet PKI Client:

- Процессор — Intel Core 2 Duo или другой схожий по производительности x86-совместимый процессор с количеством ядер 2 и более.
- Объем оперативной памяти — не менее 2 Гбайт.
- Свободное место на жестком диске — не менее 300 Мбайт.
- Операционная система — Linux, поддерживаются следующие дистрибутивы (32- и 64-разрядные):
  - Альт 8 СП Рабочая станция;
  - Альт Рабочая станция 9;
  - Альт Линукс СПТ 7.0;
  - ЛОТОС (для рабочих станций);
  - РЕД ОС 7.1 «МУРОМ», 7.2;
  - РОСА «Кобальт»;
  - Astra Linux Common Edition («Орел») 2.12;
  - Astra Linux Special Edition («Смоленск») 1.5, 1.6, в том числе в режиме замкнутой программной среды.
  - Debian 8, 9, 10;
  - Ubuntu 16.04 LTS, 18.04 LTS, 20.04 LTS;
  - Ubuntu Server 16.04 LTS, 18.04 LTS, 20.04 LTS.

    Для Ubuntu и Ubuntu Server 20.04 LTS должен быть установлен пакет `libqtgui4`.

Примечание. На некоторых дистрибутивах при использовании графической оболочки GNOME могут отсутствовать иконки программы в области уведомлений. В этом случае используйте другую графическую оболочку.

- Веб-браузер — Mozilla Firefox, Chromium последних версий.

  Для ОС должны быть установлены последние пакеты обновлений.

Обратная связь

Дополнительная информация

Сведения о продуктах и решениях ViPNet, распространенные вопросы и другая полезная информация собраны на сайте ИнфоТеКС:

- Информация о продуктах ViPNet.
- Информация о решениях ViPNet.
- Часто задаваемые вопросы.
- Форум пользователей продуктов ViPNet.

Контактная информация

Если у вас есть вопросы, свяжитесь со специалистами ИнфоТеКС:

- Единый многоканальный телефон:

  +7 (495) 737-6192,

  8-800-250-0-260 — бесплатный звонок из России (кроме Москвы).

- Служба поддержки: hotline@infotecs.ru.

  Форма для обращения в службу поддержки через сайт.

  Телефон для клиентов с расширенной поддержкой: +7 (495) 737-6196.

- Отдел продаж: soft@infotecs.ru.

Если вы обнаружили уязвимости в продуктах компании, сообщите о них по адресу security-notifications@infotecs.ru. Распространение информации об уязвимостях продуктов компании ИнфоТеКС регулируется политикой ответственного разглашения.

1

Общие сведения

Назначение

Программа File Unit устанавливается на рабочие места пользователей вместе с другими компонентами ViPNet PKI Client и предназначена для обеспечения безопасности файлов, передаваемых по открытым каналам связи или с помощью съемных носителей.

С помощью программы File Unit вы можете:

- Обеспечивать безопасность файлов с помощью шифрования (см. Зашифрование файла на стр. 37) и заверения электронной подписью (см. Заверение файла электронной подписью на стр. 34).

  Электронная подпись удостоверяет личность подписавшего файл, а также подтверждает целостность данных, содержащихся в этом файле (то есть подтверждает, что содержимое файла не изменялось после подписания).

  Шифрование обеспечивает конфиденциальность данных, содержащихся в файле. Только получатель, с использованием сертификата которого зашифрован файл, сможет расшифровать этот файл и ознакомиться с его содержимым.

  Таким образом, программа File Unit защищает файл от подделки с помощью электронной подписи, а также от получения злоумышленником конфиденциальной информации, содержащейся в файле, путем шифрования данного файла.

- Работать с зашифрованными файлами, полученными от других пользователей (см. Расшифрование файла на стр. 43).

  При получении файла, зашифрованного с использованием вашего сертификата, вы можете расшифровать его с помощью программы File Unit. При этом вы можете расшифровывать файлы, зашифрованные как с помощью программы File Unit, так и с помощью других программ, поддерживающих асимметричные алгоритмы шифрования (см. глоссарий, стр. 52) и стандартный формат `*.enc` (см. глоссарий, стр. 54) для зашифрованных файлов.

- Проверять личность отправителя и целостность полученных файлов (см. Проверка электронной подписи на стр. 45).

  При получении какого-либо подписанного файла вы можете проверить его электронную подпись, чтобы подтвердить личность отправителя и удостовериться в целостности полученных данных. При этом можно проверить электронную подпись файлов, подписанных как с помощью программы File Unit, так и с помощью других программ, поддерживающих асимметричные алгоритмы электронной подписи (см. глоссарий, стр. 52) и стандартный формат `*.sig` (см. глоссарий, стр. 54) для подписанных файлов.

  В подписанном файле `*.sig` вместе с электронной подписью передается также сертификат пользователя, подписавшего файл. Поэтому для проверки электронной подписи отдельная передача сертификата получателям файла не требуется.

- Подтверждать точное время заверения файлов электронной подписью (см. Заверение файла электронной подписью на стр. 34).

При заверении файла электронной подписью вы можете добавить к электронной подписи штамп точного времени. Штамп точного времени подтверждает точное время заверения файла электронной подписью и при возникновении спорных ситуаций позволяет доказать факт существования файла на момент его подписания.

Для выполнения криптографических операций программа File Unit использует следующие криптографические алгоритмы:

- Алгоритмы формирования и проверки электронной подписи данных ГОСТ Р 34.10-2001 (с вычислением хэш-функции по ГОСТ Р 34.11-94) и ГОСТ Р 34.10-2012 (с вычислением хэш-функции по ГОСТ Р 34.11-2012).
- Алгоритм шифрования информации ГОСТ 28147-89.

Требования к сертификатам для заверения электронной подписью и шифрования

Для заверения электронной подписью и шифрования файлов сертификаты должны удовлетворять следующим требованиям:

- Сертификат должен быть действителен:
  - Срок действия сертификата не истек.
  - Срок действия ключа ЭП не истек.
  - Сертификат не аннулирован.
  - Вся цепочка сертификации (см. глоссарий, стр. 54) полна, и все входящие в нее сертификаты удостоверяющих центров действительны.
- Для шифрования сертификаты получателей должны быть установлены в хранилище сертификатов **Другие пользователи** и иметь в поле **Использование ключа** хотя бы одно из назначений: **Шифрование данных**, **Шифрование ключей**, **Согласование ключей**.
- Для заверения файлов электронной подписью ваш сертификат должен быть установлен в хранилище сертификатов текущего пользователя **Личное** и иметь назначение **Цифровая подпись** в поле **Использование ключа**. В случае если запрос на сертификат был создан не с помощью ViPNet PKI Client, должна быть установлена связь между сертификатом и контейнером с ключом ЭП (см. документ «ViPNet CSP Linux 4.2. Руководство пользователя», раздел «Установка сертификата в системное хранилище»).

Внимание! В случае если ваш сертификат или сертификат получателя не соответствует указанным требованиям, вы не сможете выбрать его для заверения электронной подписью или шифрования.

Принцип работы

Программа File Unit выполняет формирование и проверку электронной подписи, а также шифрование и расшифрование файлов, при этом для выполнения криптографических операций программа обращается к криптопровайдеру ViPNet CSP (см. глоссарий, стр. 52).

Программа File Unit работает на основе алгоритмов асимметричного шифрования и выработки электронной подписи, которые используют пару связанных между собой асимметричных ключей пользователя:

- Ключ ЭП — используется для формирования электронной подписи и расшифрования файлов. Ключ ЭП конфиденциален и должен храниться в секрете.
- Ключ проверки ЭП — используется для проверки электронной подписи и шифрования файлов. Ключ проверки ЭП свободно распространяется среди других пользователей в составе сертификата пользователя (см. глоссарий, стр. 53).

Примечание. В федеральном законе № 63-ФЗ «Об электронной подписи» от 6 апреля 2011 г. используются термины:

- Ключ, предназначенный для создания электронной подписи, называется ключом электронной подписи (см. глоссарий, стр. 53).
- Ключ, предназначенный для проверки подлинности электронной подписи, называется ключом проверки электронной подписи (см. глоссарий, стр. 53).

Рассмотрим принцип работы программы File Unit совместно с криптопровайдером ViPNet CSP на следующих примерах:

- Заверение данных электронной подписью (на стр. 14).
- Шифрование данных (на стр. 15).
- Заверение электронной подписью и шифрование данных (на стр. 16).

Заверение данных электронной подписью

Заверение файла электронной подписью и передача его другому пользователю происходит следующим образом:

1 Пользователь **A** в программе File Unit инициирует заверение файла электронной подписью, который хочет передать пользователю **B**.

2 При заверении файла электронной подписью программа File Unit обращается к криптопровайдеру ViPNet CSP для формирования электронной подписи с помощью закрытого ключа пользователя **A**. Затем программа File Unit формирует файл с расширением `*.sig`, содержимое которого зависит от того, какой тип электронной подписи использует пользователь **A**:

- В случае использования прикрепленной подписи (см. глоссарий, стр. 53) в файл `<имя_файла>.sig` помещаются исходный файл, сформированная электронная подпись и служебная информация.

  Прикрепленная подпись обеспечивает простоту обмена, копирования и шифрования подписанных файлов (например, в системах электронного документооборота). При этом ознакомиться с содержимым файла смогут только пользователи, на компьютерах которых установлены специальные средства работы с файлами `*.sig` (программы File Unit, ViPNet Деловая почта или программы сторонних производителей со схожим функционалом, например КриптоАРМ).

- В случае использования открепленной подписи (см. глоссарий, стр. 53) в файл `<имя_файла>.detached.sig` помещаются сформированная электронная подпись и служебная информация. При этом исходный файл передается пользователю **B** отдельно (для проверки электронной подписи требуется и файл с открепленной подписью, и исходный файл).

  Открепленная подпись позволяет ознакомиться с содержимым исходного файла пользователям, на компьютерах которых не установлены средства работы с файлами `*.sig`. Однако в этом случае затрудняется передача, шифрование и другие операции с файлом подписи, так как операции необходимо производить с двумя файлами: исходным файлом и файлом `<имя_файла>.detached.sig`.

Рисунок 1. Заверение документа электронной подписью с помощью программы File Unit

3 Пользователь **A** передает пользователю **B** файл с расширением `*.sig` и исходный файл (если была выбрана открепленная подпись), например, с помощью электронной почты.

4 Пользователь **B** проверяет электронную подпись с использованием открытого ключа пользователя **A**, который входит в состав сертификата подписи.

В результате пользователь **B** сможет ознакомиться с данными, содержащимися в полученном файле, и убедиться в их подлинности.

Шифрование данных

Шифрование файла и передача его другому пользователю происходит следующим образом:

1 Отправитель в программе File Unit инициирует шифрование файла, который хочет передать нескольким получателям.

2 Отправитель из хранилища сертификатов выбирает сертификат одного или нескольких получателей, которым собирается передать зашифрованный файл.

3 При шифровании файла программа File Unit обращается к криптопровайдеру ViPNet CSP для шифрования файла с помощью открытых ключей выбранных получателей. В результате программа File Unit формирует зашифрованный файл с расширением `*.enc`.

Рисунок 2. Шифрование документа с помощью программы File Unit

4 Отправитель передает получателям зашифрованный файл, например, с помощью электронной почты.

5 Получатели расшифровывают файл с использованием своих закрытых ключей.

В результате получатели смогут ознакомиться с конфиденциальными данными, содержащимися в полученном файле.

Заверение электронной подписью и шифрование данных

Заверение электронной подписью и шифрование файла с использованием алгоритмов ГОСТ и передача его одному или нескольким пользователям осуществляются следующим образом:

1 Отправитель в программе File Unit инициирует заверение электронной подписью и шифрование файла, который хочет передать другим пользователям (получателям).

2 При заверении файла электронной подписью программа File Unit обращается к криптопровайдеру ViPNet CSP для формирования электронной подписи с помощью закрытого ключа отправителя. Затем программа File Unit формирует файл с расширением `*.sig`:

   - В случае использования прикрепленной подписи в файл `<имя_файла>.sig` помещаются исходный файл, сформированная электронная подпись и служебная информация.
   - В случае использования откреплennой подписи в файл `<имя_файла>.detached.sig` помещаются сформированная электронная подпись и служебная информация. При этом исходный файл не помещается в файл `<имя_файла>.detached.sig`.

3 Отправитель из хранилища сертификатов выбирает сертификат одного или нескольких получателей, которым собирается передать зашифрованный и подписанный файл.

4. При шифровании файла программа File Unit обращается к криптопровайдеру ViPNet CSP для шифрования файла с помощью открытых ключей выбранных получателей. В результате программа File Unit формирует зашифрованный файл с расширением `*.enc`.
5. Отправитель передает получателям файл с зашифрованными и подписанными данными, например, с помощью электронной почты.
6. Получатели расшифровывают файл с использованием своих закрытых ключей.
7. Получатели проверяют электронную подпись с использованием открытого ключа отправителя, который входит в состав сертификата подписи.

В результате получатели смогут ознакомиться с данными, которые содержатся в полученном файле.

2

Начало работы

Установка

Программа File Unit входит в состав ViPNet PKI Client, она устанавливается в процессе развертывания этого комплекса.

Для установки ViPNet PKI Client следуйте рекомендациям, приведенным в документе «ViPNet PKI Client Linux. Руководство администратора» в разделе «Установка и обновление».

Запуск

Чтобы запустить программу File Unit, в меню приложений выберите  **ViPNet PKI Client File Unit** или выполните команду:

```
/opt/itcs/bin/pki-client-file-unit
```

Чтобы перейти к настройкам компонентов ViPNet PKI Client, выполните одно из действий:

- В основном окне программы File Unit нажмите кнопку  **Настройки**.
- В меню приложений выберите  **ViPNet PKI Client Settings**.
- Выполните команду:

  ```
  /opt/itcs/bin/pki-client-settings
  ```

Интерфейс

Главное окно программы File Unit представлено на рисунке ниже.

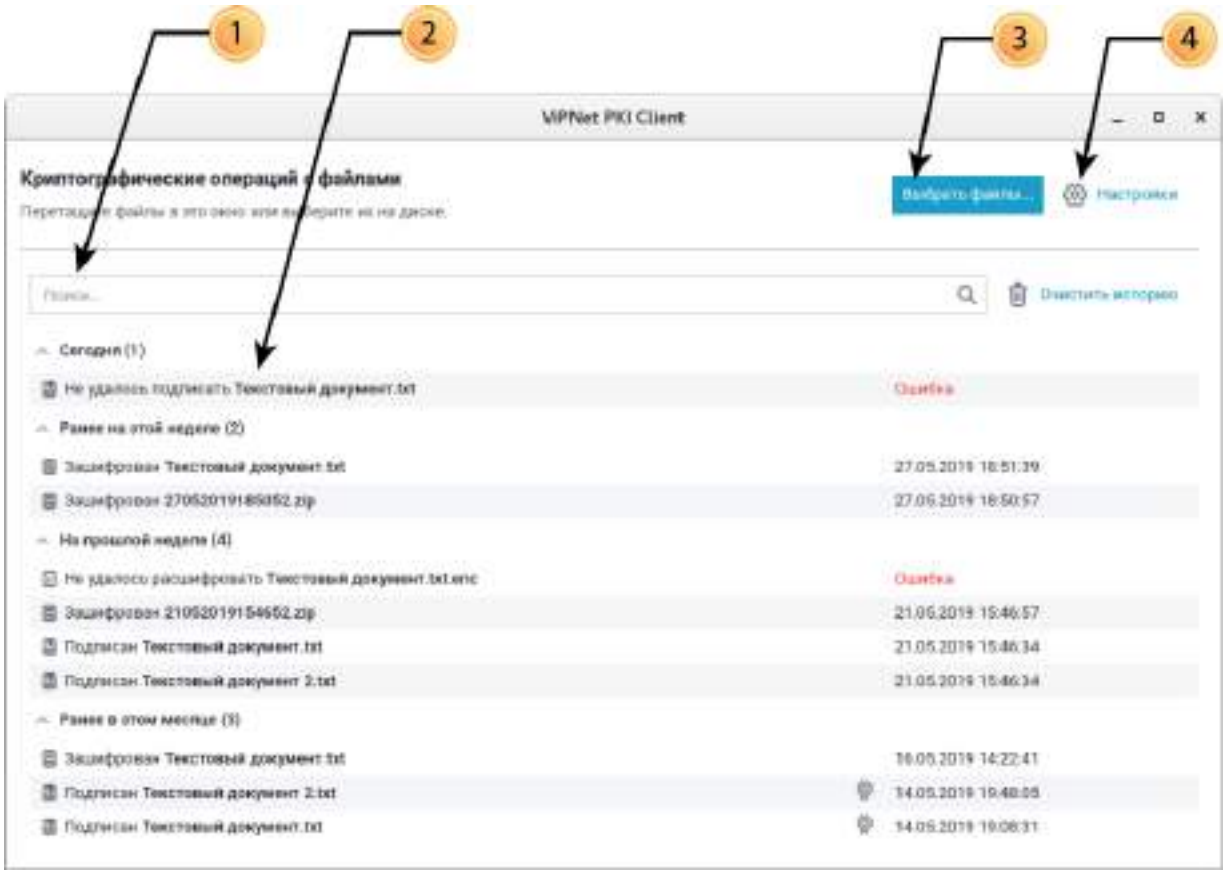

Рисунок 3. Интерфейс программы File Unit

Цифрами на рисунке обозначены:

1. Строка поиска файлов.
2. Область истории операций с файлами.
3. Кнопка выбора файлов для выполнения криптографических операций.
4. Кнопка настройки.

3

Подготовка к работе с файлами

Порядок действий при подготовке к работе

Таблица 3. Порядок действий

	Действие
☐	Подготовьте личный сертификат и ключ ЭП (на стр. 24)
☐	Установите сертификаты издателей и CRL в хранилище сертификатов (на стр. 28)
☐	Настройте параметры электронной подписи (на стр. 32)
☐	Настройте параметры шифрования файлов (на стр. 36)

Подготовка личного сертификата и ключа ЭП

У меня нет сертификата и ключа ЭП

1 Создайте запрос на сертификат (см. Получение нового сертификата на стр. 26).

2 Передайте запрос в УЦ и получите личный сертификат, сертификат издателя и CRL, а если ваш УЦ не является корневым, все сертификаты издателей из цепочки сертификации и соответствующие CRL.

3 Установите личный сертификат в хранилище сертификатов (на стр. 28).

У меня есть сертификат и ключ ЭП в папке на диске

Примечание. Этот вариант подходит, если у вас имеется 1 файл: контейнер ключей, включающий сертификат, или 2 файла: контейнер ключей и сертификат.

Если ваш сертификат и ключ ЭП хранятся в файле PFX, следуйте указаниям раздела Перенос сертификатов и ключей ЭП между компьютерами.

---

1 Скопируйте контейнер ключей в каталог `/home/<user name>/.itcs/vipnet-csp/containers`.

2 Перейдите в каталог `/opt/itcs/bin` и запустите утилиту `certmgr-gui`.

3 В окне **Хранилище сертификатов** выберите хранилище **Текущий пользователь**  .

4 На левой панели выберите раздел **Личное (My)** и на панели инструментов нажмите **Импорт**  .

5 Если у вас имеется только контейнер ключей:

5.1 Установите переключатель в положение **Сертификат из контейнера ключей** и выберите контейнер ключей. Нажмите **Далее**.

5.2 Пропустите остальные шаги и завершите работу мастера.

6 Если у вас имеется контейнер ключей и сертификат:

6.1 Установите переключатель в положение **Сертификат или CRL на диске** и выберите файл сертификата. Нажмите **Далее**.

6.2 В списке выберите контейнер ключей. Нажмите **Далее**.

6.3 Завершите работу мастера.

У меня есть сертификат и ключ ЭП на внешнем устройстве (токене)

1 Подключите внешнее устройство к компьютеру.

2 Перейдите в раздел  **Подключено устройств**, нажмите в строке сертификата и в меню выберите **Установить в хранилище**.

Получение нового сертификата

Чтобы выполнять криптографические операции, вам необходимо иметь контейнер ключей и сертификат. Сертификат издается удостоверяющим центром по вашему запросу, в котором указываются необходимые данные. Контейнер ключей и сертификат могут храниться в папке на диске или внешнем устройстве (токене).

Чтобы создать запрос на сертификат:

1 Перейдите в настройки ViPNet PKI Client (на стр. 20) и в разделе **Сертификаты** и нажмите **Создать запрос**.

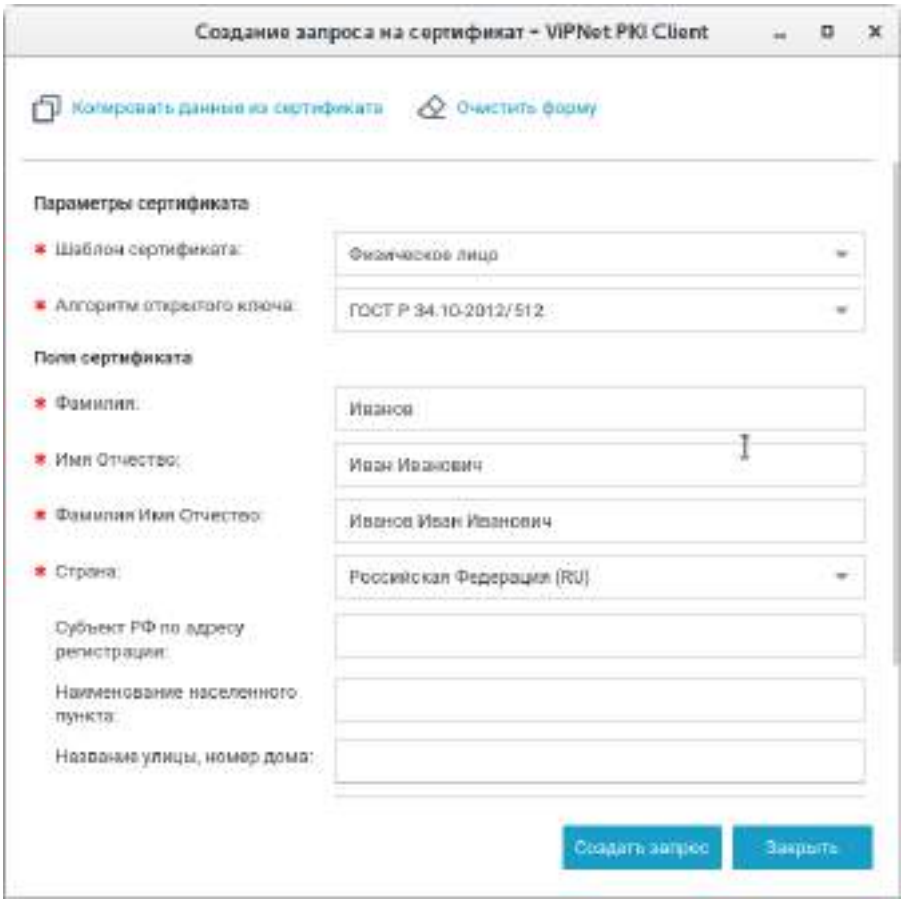

Рисунок 4. Создание запроса на сертификат

Примечание. Если у вас есть сертификат, вы можете создать запрос на его основе. Для этого нажмите **Копировать данные из сертификата** и выберите сертификат для автоматического заполнения полей. Если нужно, измените информацию в полях запроса вручную.

---

2 Выберите **Шаблон** сертификата. В каждом шаблоне содержится разное количество и наименование атрибутов, которые попадут в поле сертификата **Субъект (Subject)**.

3 Выберите **Алгоритм открытого ключа** или оставьте значение по умолчанию.

4 Заполните поля и нажмите **Создать запрос**.

5 Укажите имя и папку для сохранения файла запроса и нажмите **Сохранить**.

6 В окне **ViPNet CSP — инициализация контейнера ключей:**

- Укажите имя и место для сохранения контейнера ключей (см. глоссарий, стр. 53).
- Задайте пароль для работы с контейнером ключей.

7 В окне **Электронная рулетка** отобразится процесс инициализации генератора случайных чисел. Следуйте указаниям в этом окне.

8 В окне сообщения об успешном создании файла запроса нажмите кнопку **OK**.

9 Передайте запрос в УЦ и получите личный сертификат, сертификат издателя и CRL, а если ваш УЦ не является корневым, все сертификаты издателей из цепочки сертификации и соответствующие CRL.

После получения сертификата установите его в хранилище (см. Установка сертификатов и CRL на стр. 28).

Установка сертификатов и CRL

Указанным способом устанавливайте только те личные сертификаты, запрос на которые был создан в ViPNet PKI Client (см. Получение нового сертификата на стр. 26). Если вы получали сертификат иным способом, следуйте указаниям раздела Подготовка личного сертификата (на стр. 24).

ViPNet PKI Client также поддерживает работу с файлами формата PKSC#7. Установка сертификатов из таких файлов осуществляется аналогично. Если файл формата PKSC#7 помимо сертификатов содержит CRL, они также могут быть установлены в хранилище сертификатов.

Чтобы установить сертификаты и (или) CRL:

1 Перейдите в настройки ViPNet PKI Client (на стр. 20).

Внимание! Чтобы установить сертификаты издателей и CRL в хранилище локального компьютера, запустите настройки ViPNet PKI Client с правами суперпользователя. В этом случае не устанавливайте личные сертификаты и сертификаты получателей, поскольку они будут установлены в хранилище сертификатов пользователя root и вы не сможете работать с ними после запуска настроек под своей учетной записью.

---

2 В разделе  **Сертификаты** нажмите  **Добавить сертификат или CRL** и укажите путь к файлу сертификата или CRL.

3 В окне **Добавление сертификатов и CRL** отображаются устанавливаемые сертификаты и (или) CRL.

Сертификаты и CRL с истекшим сроком действия или имеющие недействительную цифровую подпись отмечаются значком  .

При необходимости вы можете:

- Установить в контейнер ключей сертификат, запрос на который был создан в ViPNet PKI Client. Для этого в окне **Добавление сертификатов и CRL** установите соответствующий флажок.
- Посмотреть подробную информацию об устанавливаемых сертификатах и CRL, для этого щелкните имя владельца сертификата или CRL.
- Удалить сертификат или CRL из списка, для этого щелкните значок  (появляется при наведении курсора на строку сертификата или CRL).

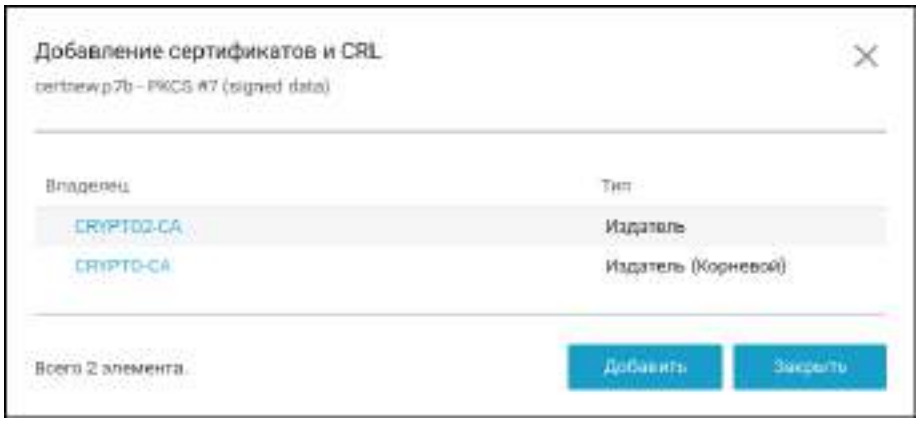

Рисунок 5. Установка сертификатов и CRL

4 В окне **Добавление сертификатов** нажмите **Добавить**, а затем **Закрыть**.

Результат установки отмечается значком напротив каждого установленного сертификата и CRL.

Примечание. Если после установки сертификата в строке имени владельца сертификата появится предупреждающее сообщение, наведите курсор на значок ⚠, просмотрите более подробные сведения об ошибках и устраните их (см. Предупреждающие сообщения на стр. 30).

Рисунок 6. Просмотр предупреждающих сообщений

Предупреждающие сообщения

Предупреждающие сообщения предназначены для информирования пользователя о невозможности использования установленных сертификатов для выполнения криптографических операций (заверения электронной подписью, шифрования, расшифрования).

Во время установки сертификатов ViPNet PKI Client выполняет проверку сертификатов на соответствие следующим требованиям:

- Срок действия сертификата не истек.
- Сертификат не находится в списке аннулированных сертификатов доверенного удостоверяющего центра.
- Цепочка сертификации (см. глоссарий, стр. 54) полна, и все входящие в нее сертификаты удостоверяющих центров действительны.

Вы можете выполнить проверку установленных сертификатов вручную. Для этого:

1 Перейдите в настройки ViPNet PKI Client (на стр. 20) и выберите раздел  **Сертификаты**.

2 На панели инструментов нажмите  .

В случае если устанавливаемый сертификат не соответствует указанным требованиям, в строке имя владельца сертификата появится предупреждающее сообщение (см. рисунок на стр. 29):

- **Ошибка построения цепочки сертификатов**

  Установите в хранилище все сертификаты, образующие цепочку сертификации (на стр. 28).

- **Сертификат отозван**

  Получите новый сертификат (см. Получение нового сертификата на стр. 26) и установите его в хранилище (см. Установка сертификатов и CRL на стр. 28).

- **Подпись неверна**

  Сертификат или один из сертификатов, образующих цепочку сертификации, искажен. Переустановите все сертификаты, образующие цепочку сертификации.

- **Срок действия ключа электронной подписи истек**

  - Если вы устанавливаете личный сертификат, получите новый сертификат (см. Получение нового сертификата на стр. 26) и установите его в хранилище (см. Установка сертификатов и CRL на стр. 28).
  - Если вы устанавливаете сертификат получателя, запросите у получателя новый сертификат.

- **Статус отзыва не определен**

  При появлении данного предупреждающего сообщения установите актуальный CRL в хранилище сертификатов (на стр. 28).

4

Обеспечение безопасности файлов с помощью электронной подписи и шифрования

Подтверждение личности отправителя с помощью электронной подписи

Данные, передаваемые по открытым каналам связи, могут быть повреждены или подменены злоумышленником. Чтобы избежать искажения данных посторонними лицами, в ViPNet PKI Client реализован механизм электронной подписи. Электронная подпись позволяет:

- Определить лицо, подписавшее документ.
- Обнаружить факт искажения данных, содержащихся в документе, произошедший после момента заверения электронной подписью.

Чтобы заверить документ своей электронной подписью:

1 Убедитесь, что у вас есть сертификат и соответствующий ключ ЭП (на стр. 24).

2 Если ваш сертификат установлен в хранилище сертификатов, проверьте, что в хранилище также установлены сертификаты издателей и соответствующие CRL (на стр. 28).

3 Настройте параметры электронной подписи (см. Настройка параметров электронной подписи на стр. 32).

4 Заверьте файл электронной подписью (см. Заверение файла электронной подписью на стр. 34).

5 Передайте подписанный файл получателям любым удобным способом.

Настройка параметров электронной подписи

Настройте параметры электронной подписи, которые будут использоваться по умолчанию в программах File Unit и Web Unit. Для этого:

1 Перейдите в настройки ViPNet PKI Client (на стр. 20).

2 В разделе  **Подпись** нажмите  **Выберите сертификат**.

3 Выберите сертификат и нажмите **Выбрать**.

Отобразится информация о выбранном сертификате. Для просмотра подробной информации об используемом сертификате щелкните имя владельца сертификата.

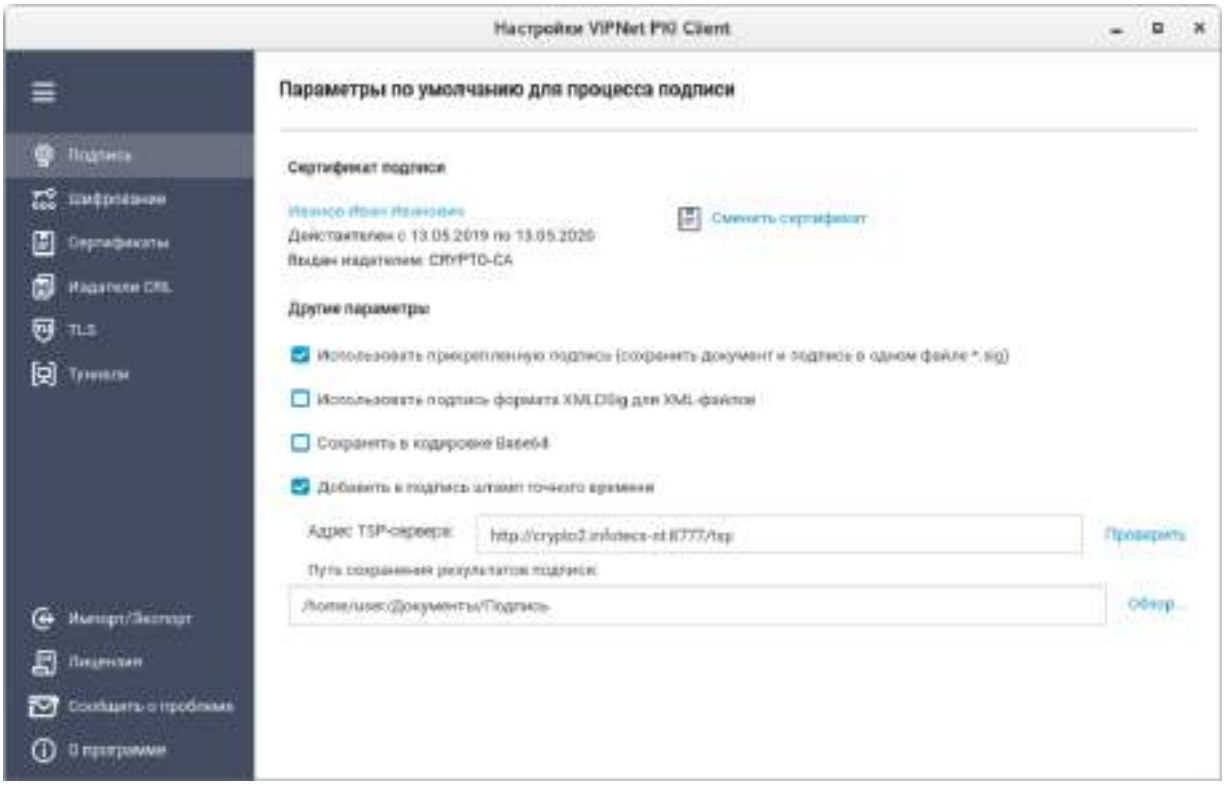

Рисунок 7. Настройка параметров электронной подписи

4 Чтобы сохранять подпись отдельно от подписываемого файла (см. глоссарий, стр. 53), снимите флажок **Использовать прикрепленную подпись (сохранить документ и подпись в одном файле *.sig)**. По умолчанию подпись прикрепляется к подписываемому файлу.

5 Чтобы использовать подпись формата XMLDSig (см. глоссарий, стр. 52) для XML-файлов, установите соответствующий флажок и выберите шаблон. По умолчанию в настройки добавлен шаблон с параметрами:

- Подписывается весь XML-документ, подпись помещается в корневой тег.
- Алгоритм каноникализации — `http://www.w3.org/TR/2001/REC-xml-c14n-20010315`.
- Алгоритм трансформации — `http://www.w3.org/2000/09/xmldsig#enveloped-signature`.

Если этот шаблон не подходит, создайте свой и импортируйте его в настройки.

6 Чтобы сохранять файл подписи в кодировке Base64, установите соответствующий флажок.

7 Чтобы добавлять к электронной подписи подтверждение точного времени заверения файла, настройте подключение к службе штампов времени (см. глоссарий, стр. 54). Для этого:

7.1 Установите флажок **Добавить в подпись штамп точного времени**.

7.2 В поле **Адрес TSP-сервера** укажите URL-адрес TSP-сервера (см. глоссарий, стр. 52) в формате `http://<IP-адрес или доменное имя>:<порт>/`. Для проверки соединения с указанным TSP-сервером нажмите **Проверить**. Поддерживается только протокол HTTP.

8 Чтобы все подписанные файлы по умолчанию сохранялись в определенной папке, в соответствующем поле с помощью кнопки **Обзор** укажите путь к нужной папке. Если папка по

умолчанию не будет указана, то подписанные файлы будут сохраняться в папку `/home/<имя пользователя>`.

9 Нажмите кнопку **Сохранить**.

Заверение файла электронной подписью

С помощью программы File Unit вы можете заверить файл своей электронной подписью, которая удостоверяет личность отправителя файла и целостность содержащихся в нем данных. Для этого:

1 В главном окне программы (см. рисунок на стр. 21) выполните одно из действий:

- Нажмите **Выбрать файлы** и выберите один или несколько файлов.
- Перетащите файлы в главное окно программы.

Примечание. Чтобы открыть документ, который вы собираетесь заверить электронной подписью, щелкните название этого документа в разделе **Выбранные файлы**.

---

2 В разделе **Доступные операции** установите флажок **Подписать сертификатом**.

Станут доступны настройки параметров электронной подписи.

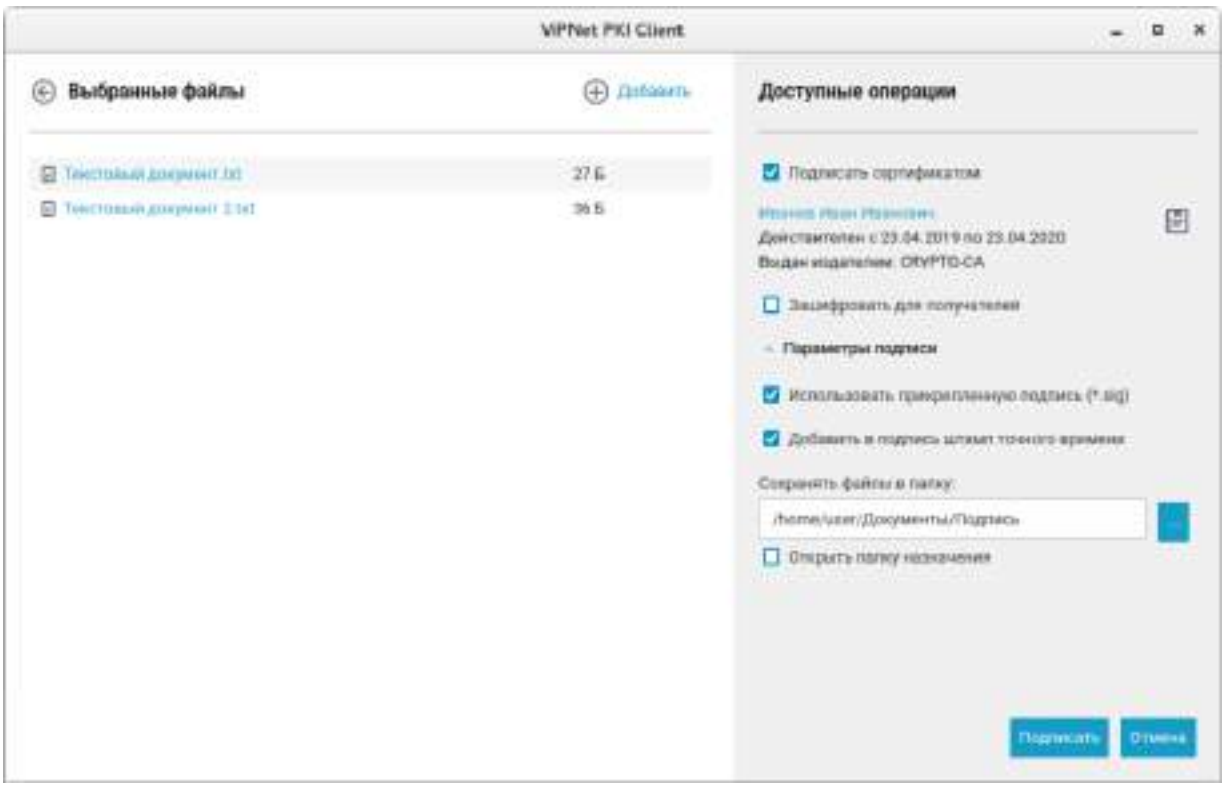

Рисунок 8. Заверение файла электронной подписью

3 Если необходимо, измените параметры электронной подписи и нажмите **Подписать**.

4 В окне ввода пароля, в зависимости от места хранения вашего контейнера ключей, введите:

- Пароль контейнера ключей — папка на диске.
- ПИН-код внешнего устройства — внешнее устройство.

Внимание! Допускается не более десяти попыток ввода пароля. После десяти неудачных попыток ввода пароля выполнение криптографических операций будет заблокировано на 15 минут. При вводе верного пароля счетчик, который фиксирует неудачные попытки, обнуляется.

Во время блокировки не завершайте работу программы File Unit.

5 Дождитесь завершения процесса подписания файлов.

В результате будут сформированы и помещены в выбранную папку файлы:

- `<имя файла>.sig`, если вы использовали прикрепленную подпись;
- `<имя файла>.detached.sig`, если вы использовали открепленную подпись.

По окончании заверения файлов электронной подписью в области истории операций с файлами появятся соответствующие записи.

Обеспечение безопасности файлов с помощью шифрования

Передаваемые по открытым каналам данные могут быть перехвачены, искажены либо подменены злоумышленниками. Чтобы обеспечить безопасность данных с помощью программы File Unit и передать их другим пользователям:

1 Настройте параметры шифрования (см. Настройка параметров шифрования на стр. 36).

2 Зашифруйте файл (см. Зашифрование файла на стр. 37).

3 Передайте файл получателям любым удобным способом.

Настройка параметров шифрования

Настройте параметры шифрования, которые будут использоваться по умолчанию в программах File Unit и Web Unit. Для этого:

1 Обменяйтесь сертификатами с пользователями, которым вы хотите передавать зашифрованные файлы, например, с помощью электронной почты или съемных носителей.

2 Установите полученные сертификаты в хранилище (см. Установка сертификатов и CRL на стр. 28).

3 Перейдите в настройки ViPNet PKI Client (на стр. 20) и выберите раздел  **Шифрование**.

4 Чтобы каждый раз при шифровании файлов не приходилось выбирать сертификат получателя, сформируйте список получателей файлов. Для этого:

4.1 В группе **Получатели зашифрованных файлов** нажмите  **Добавить**.

4.2 Выберите сертификат и нажмите **Выбрать**.

4.3 Аналогичным образом добавьте сертификаты других получателей.

Чтобы удалить сертификат получателя из списка, щелкните значок  .

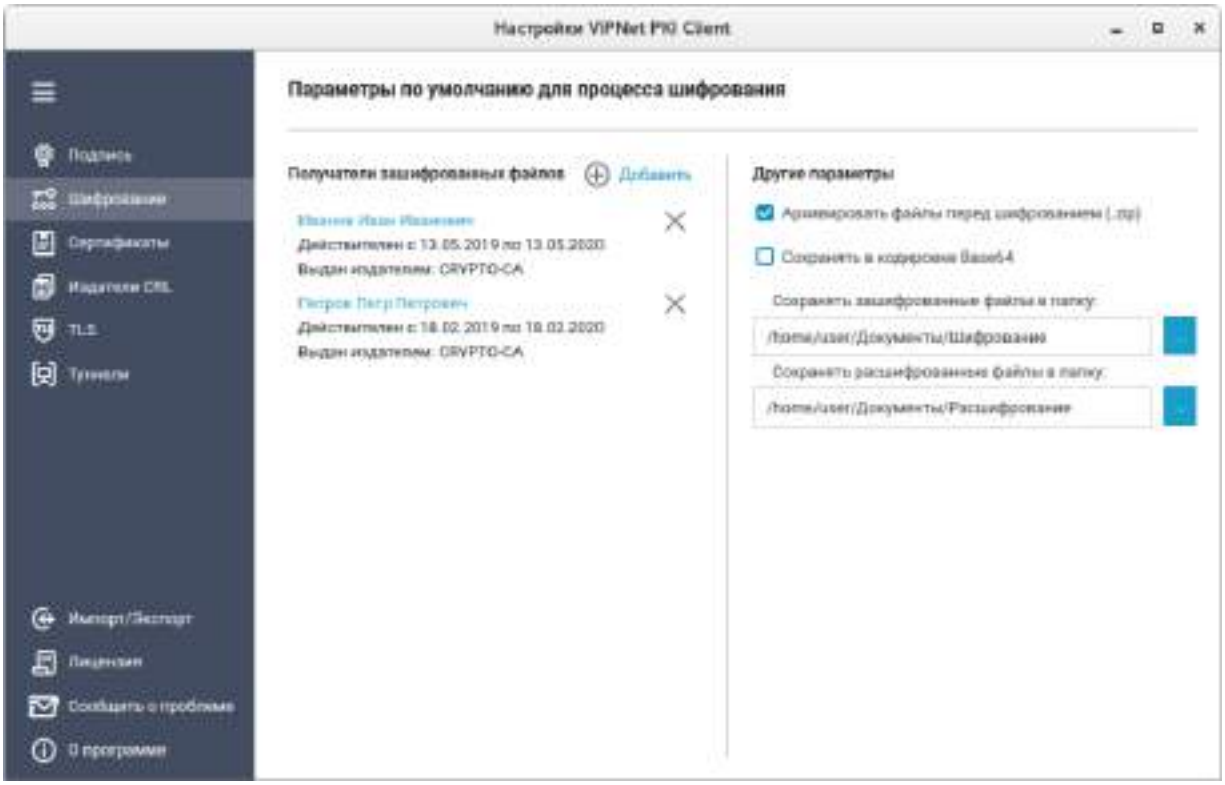

Рисунок 9. Настройка параметров шифрования

5 Чтобы перед шифрованием файлы помещались в архив, установите соответствующий флажок.

6 Чтобы сохранять зашифрованные файлы в кодировке Base64, установите соответствующий флажок.

7 С помощью кнопок ... укажите папки для сохранения зашифрованных и расшифрованных файлов.

8 Нажмите кнопку **Сохранить**.

В результате будут настроены параметры шифрования файлов.

Зашифрование файла

С помощью программы File Unit вы можете зашифровать файл с использованием сертификатов получателей (одного или нескольких). Содержимое зашифрованного файла конфиденциально, и только получатель сможет ознакомиться с ним, расшифровав файл с использованием своего закрытого ключа. Если файл зашифрован с использованием нескольких сертификатов получателей, то каждый из получателей сможет расшифровать его.

Чтобы зашифровать файл:

1 В главном окне программы (см. рисунок на стр. 21) выполните одно из действий:

- Нажмите **Выбрать файлы**. В открывшемся окне выберите один или несколько файлов и нажмите кнопку **Открыть**.

- Перетащите файлы в главное окно программы.

Примечание. Чтобы открыть документ, который вы собираетесь зашифровать, щелкните название этого документа в разделе **Выбранные файлы**.

---

2 В разделе **Доступные операции** установите флажок **Зашифровать для получателей**.

Станут доступны настройки параметров шифрования.

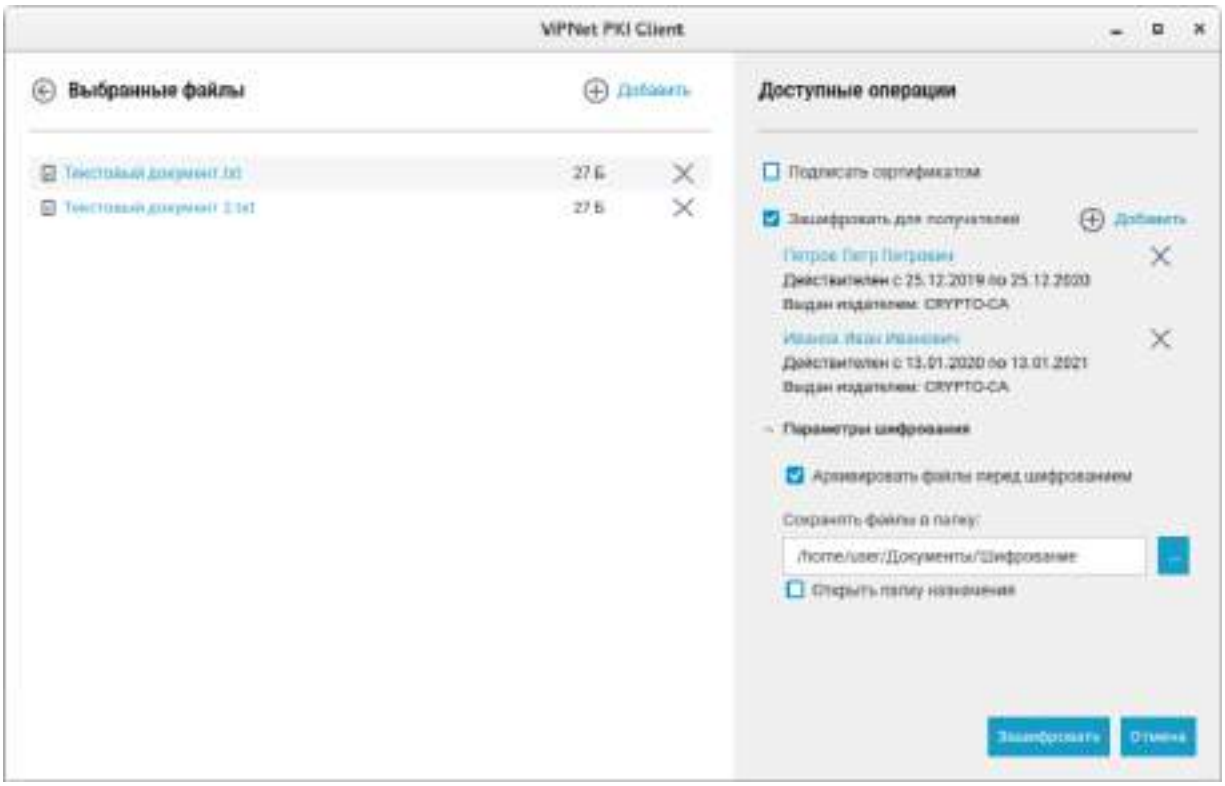

Рисунок 10. Зашифрование файла

3 Если необходимо, измените параметры шифрования и нажмите **Зашифровать**.

4 Дождитесь завершения процесса шифрования.

В результате будут сформированы зашифрованные файлы с расширением `*.enc` и помещены в выбранную папку.

Заверение электронной подписью и зашифрование файла

Если вы хотите не только подтвердить личность отправителя, но и обеспечить конфиденциальность содержимого файла, вы можете одновременно заверить файл электронной подписью и зашифровать его.

Чтобы заверить электронной подписью и зашифровать файл:

1 Запустите программу File Unit (на стр. 20).

2 В главном окне программы (см. рисунок на стр. 21) выполните одно из действий:

- Нажмите **Выбрать файлы** и выберите один или несколько файлов.
- Перетащите файлы в главное окно программы (см. рисунок на стр. 21).

Примечание. Чтобы открыть документ, который вы собираетесь заверить электронной подписью и зашифровать, щелкните название этого документа в разделе **Выбранные файлы**.

---

3 В разделе **Доступные операции** установите флажки **Подписать сертификатом** и **Зашифровать для получателей**.

Станут доступны настройки параметров электронной подписи и шифрования.

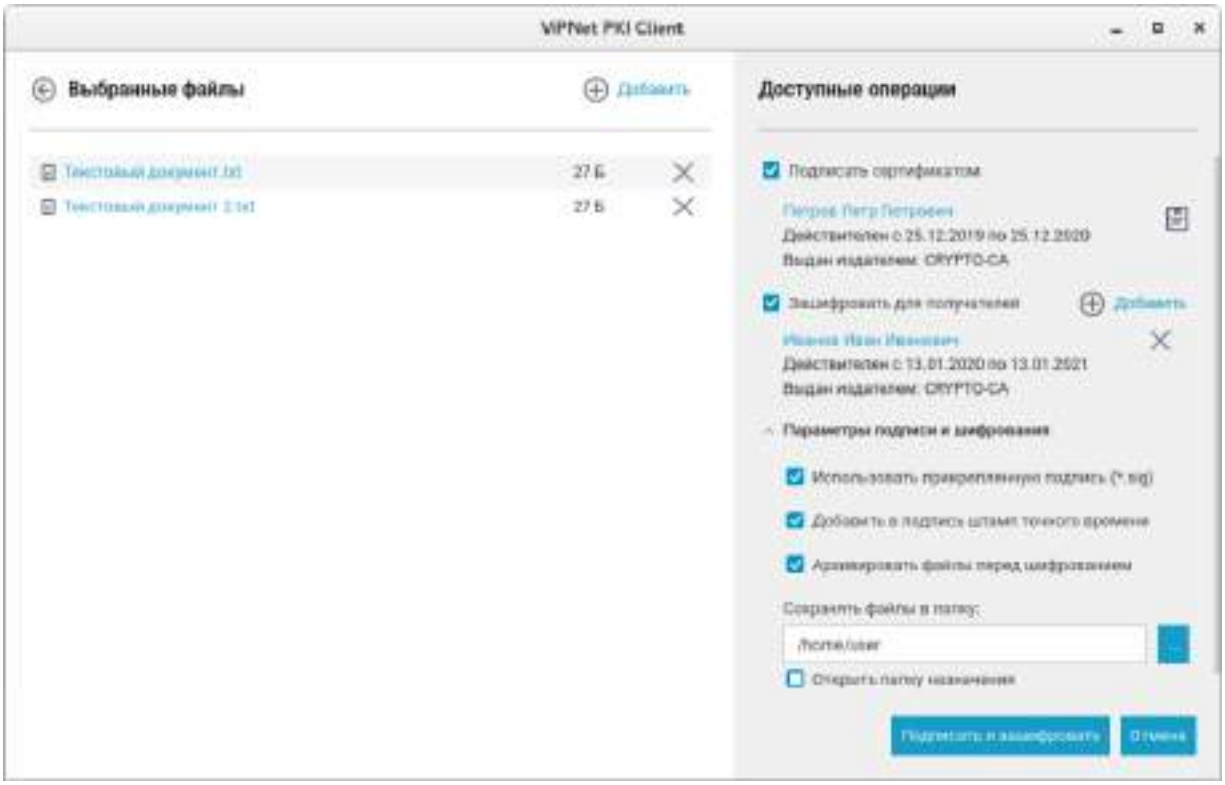

Рисунок 11. Одновременное заверение электронной подписью и шифрование файла

4 Если необходимо, измените параметры электронной подписи и шифрования и нажмите **Подписать и зашифровать**.

5 В окне ввода пароля, в зависимости от места хранения вашего контейнера ключей, введите:

- Пароль контейнера ключей — папка на диске.
- ПИН-код внешнего устройства — внешнее устройство.

Внимание! Допускается не более десяти попыток ввода пароля. После десяти неудачных попыток ввода пароля выполнение криптографических операций будет заблокировано на 15 минут. При вводе верного пароля счетчик, который фиксирует неудачные попытки, обнуляется.

Во время блокировки не завершайте работу программы File Unit.

---

6 Дождитесь завершения процесса заверения электронной подписью и шифрования файлов.

В результате будут сформированы и помещены в выбранную папку файлы:

- `<имя файла>.sig.enc`, если вы использовали прикрепленную подпись;
- `<имя файла>.detached.sig` и файл электронной подписи `<имя файла>.enc`, если вы использовали открепленную подпись без архивирования файлов перед шифрованием;
- `<ГГГГММДДччмм>.zip.sig`, если вы использовали открепленную подпись с архивированием файлов перед шифрованием. Файлы электронной подписи и исходные файлы будут содержаться в архиве `*.zip`.

5

Работа с файлами, полученными от других пользователей

Получение зашифрованных и подписанных файлов

При получении файлов, имеющих стандартные расширения `*.sig` и `*.enc`, от других пользователей с помощью программы File Unit вы можете ознакомиться с их содержимым и удостоверить личность отправителя.

В файлы с расширением `*.sig` с электронной подписью (прикрепленной (см. глоссарий, стр. 53) или открепленной (см. глоссарий, стр. 53)) помещаются также сертификаты отправителей, подписавших файл. Поэтому для проверки электронной подписи отдельно получать сертификаты других пользователей не требуется.

Чтобы ознакомиться с содержимым полученного файла, по расширению файла определите, какие операции были применены к нему перед отправкой: заверение электронной подписью, шифрование или обе операции. От этого зависит выбор операции, с помощью которой вы сможете ознакомиться с содержимым файла:

- Если файл зашифрован, то есть имеет расширение `*.enc`, расшифруйте его (см. Расшифрование файла на стр. 43).
- Если файл заверен электронной подписью, то есть имеет расширение `*.sig`, проверьте электронную подпись (см. Проверка электронной подписи на стр. 45).
- Если файл заверен электронной подписью и зашифрован, то есть имеет вид `<имя файла>.sig.enc`, то выполните расшифрование (см. Расшифрование файла на стр. 43), а затем проверку электронной подписи (см. Проверка электронной подписи на стр. 45).

Расшифрование файла

С помощью программы File Unit вы можете расшифровать полученный от другого пользователя файл, который был зашифрован с использованием вашего сертификата. Для этого:

1 В главном окне программы (см. рисунок на стр. 21) выполните одно из действий:

- Нажмите кнопку **Выбрать файлы**. В открывшемся окне выберите файл с расширением `*.enc` и нажмите кнопку **Открыть**.
- Перетащите файл с расширением `*.enc` в главное окно программы.

Файл появится в разделе **Выбранные файлы**.

2 Если файл зашифрован с помощью нескольких ваших личных сертификатов, в группе **Расшифровать используя сертификат** с помощью кнопки выберите сертификат для расшифрования.

3 При необходимости измените параметры расшифрования и нажмите **Расшифровать**.

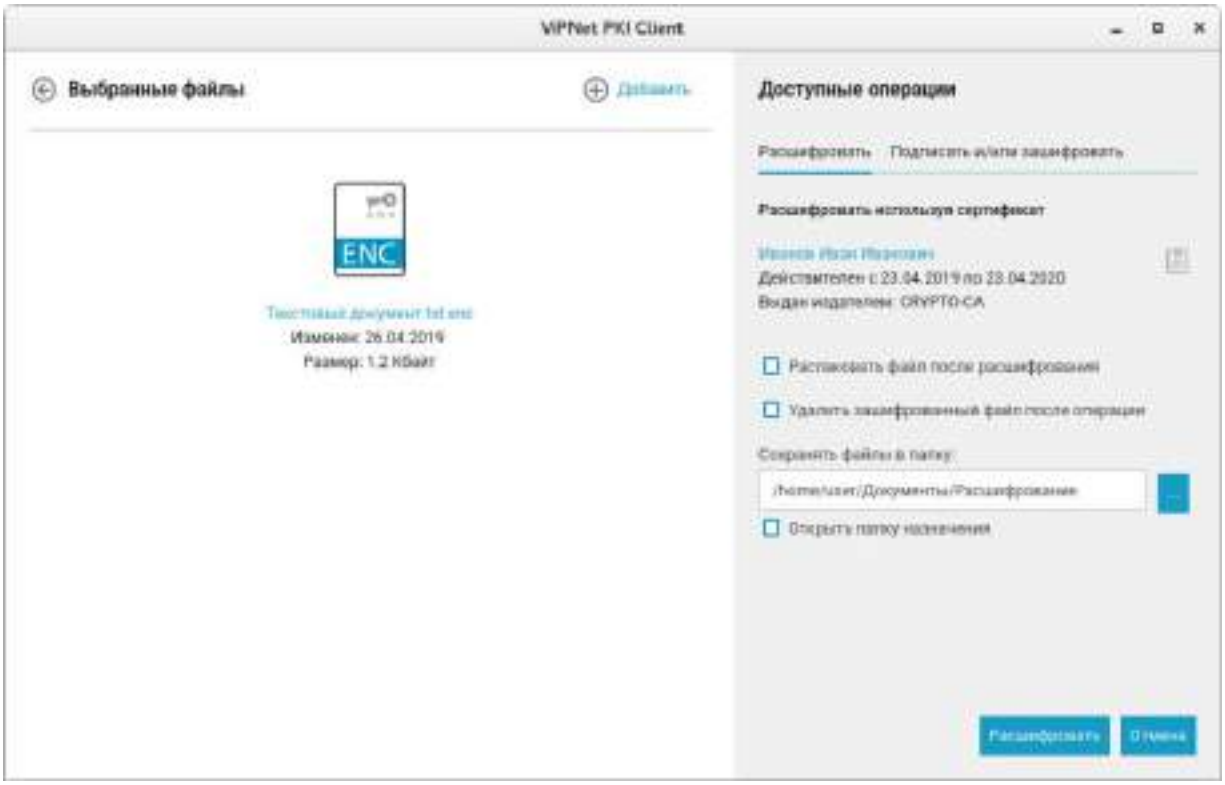

Рисунок 12. Расшифрование файла

4 В окне ввода пароля, в зависимости от места хранения вашего контейнера ключей, введите:

- Пароль контейнера ключей — папка на диске.
- ПИН-код внешнего устройства — внешнее устройство.

Внимание! Допускается не более десяти попыток ввода пароля. После десяти неудачных попыток ввода пароля выполнение криптографических операций будет заблокировано на 15 минут. При вводе верного пароля счетчик, который фиксирует неудачные попытки, обнуляется.

Во время блокировки не завершайте работу программы File Unit.

В результате файл будет расшифрован и помещен в выбранную папку.

Проверка электронной подписи

Чтобы проверить электронную подпись файлов, полученных от других пользователей:

1 Запустите программу File Unit (на стр. 20).

2 В главном окне программы (см. рисунок на стр. 21) выполните одно из действий:

Примечание. При выборе нескольких файлов проверка открепленной электронной подписи возможна, только если исходный файл расположен в той же папке, что и файл `*.detached.sig`.

- Нажмите **Выбрать файлы** и выберите один или несколько файлов с расширением `*.sig`.
- Перетащите нужные файлы с расширением `*.sig` в главное окно программы.

3 В зависимости от количества выбранных файлов и типа электронной подписи:

- Если вы выбрали один файл с прикрепленной электронной подписью, результат проверки электронной подписи будет отображен в разделе **Выбранные файлы**.

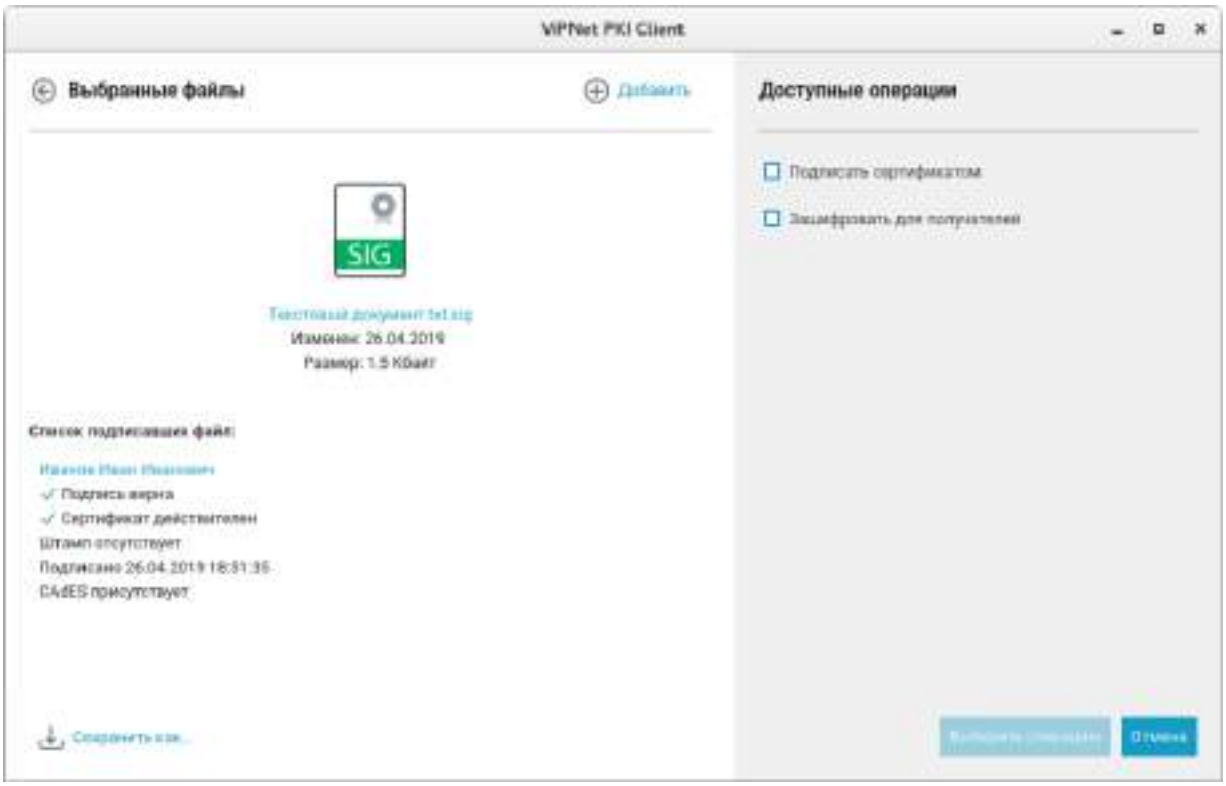

Рисунок 13. Проверка прикрепленной электронной подписи

- Если вы выбрали один файл с открепленной электронной подписью (то есть исходный файл не был помещен совместно с электронной подписью в файл `*.sig`), укажите исходный файл с помощью соответствующей кнопки или перетащите его в выделенную область.

Примечание. Если исходный файл и файл подписи расположены в одной папке, проверка электронной подписи произойдет автоматически.

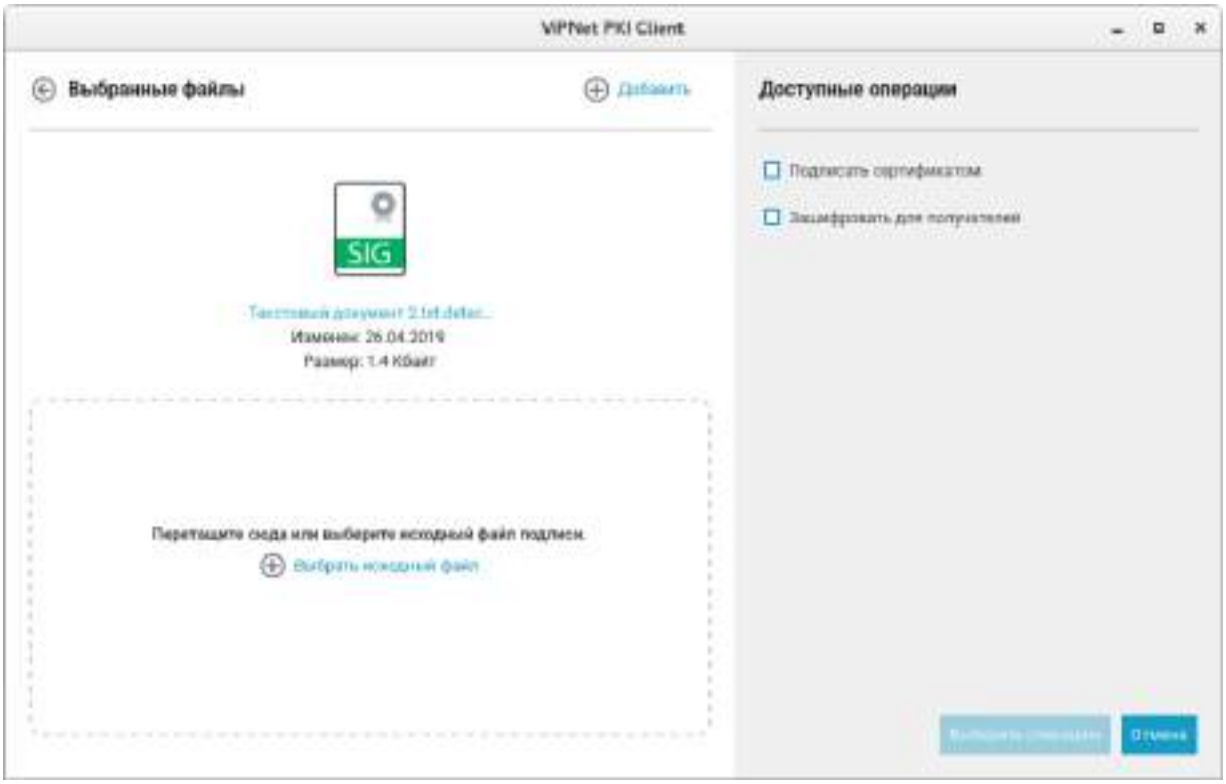

Рисунок 14. Проверка открепленной электронной подписи

- Если вы выбрали несколько файлов, то для проверки электронной подписи щелкните значок напротив имени файла. Результат проверки подписи будет отображен в отдельном окне.

Примечание. Значок не отображается у файлов с открепленной электронной подписью, если исходный файл и файл подписи расположены в разных папках. В этом случае проверку электронной подписи необходимо выполнять по одному файлу.

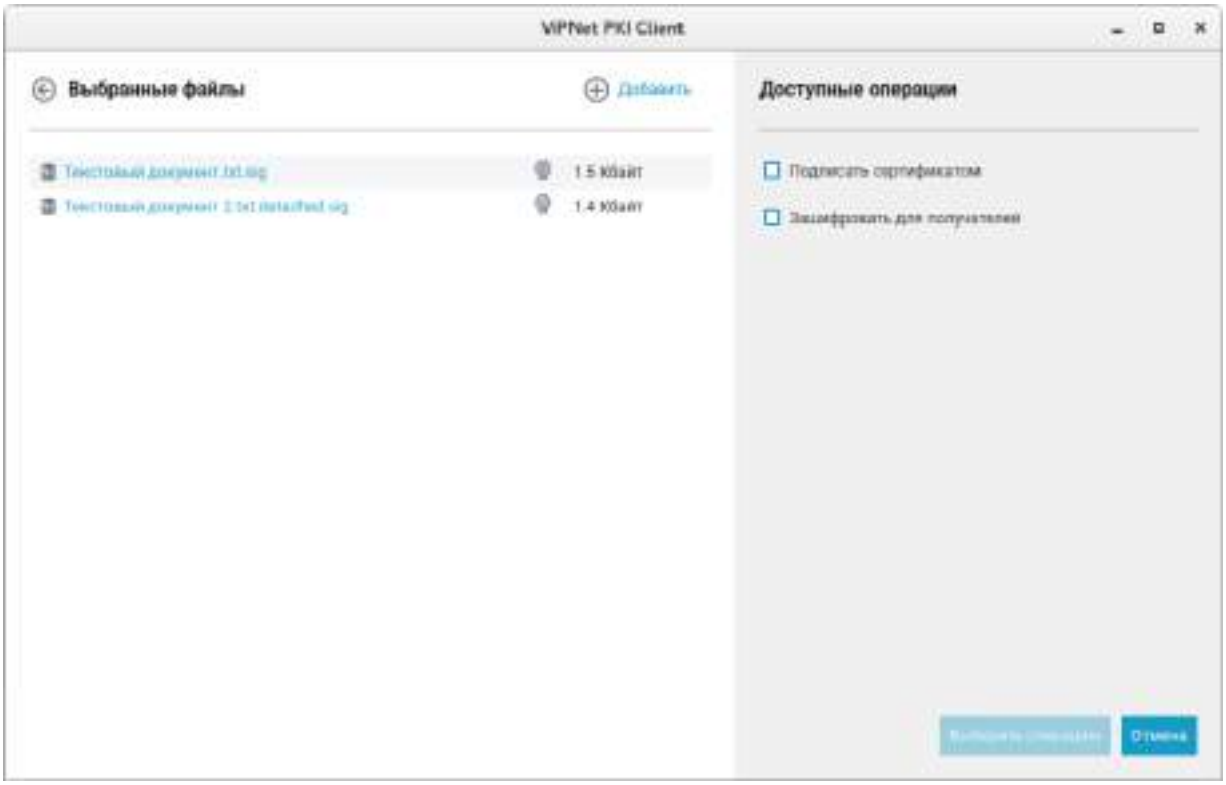

Рисунок 15. Проверка электронной подписи нескольких файлов

4 В окне с результатами проверки подписи:

- Щелкните имя владельца подписи, чтобы просмотреть информацию о его сертификате.
- Если к подписи был добавлен штамп времени, щелкните ссылку **присутствует**, чтобы просмотреть информацию о нем.
- Сохраните исходный файл.

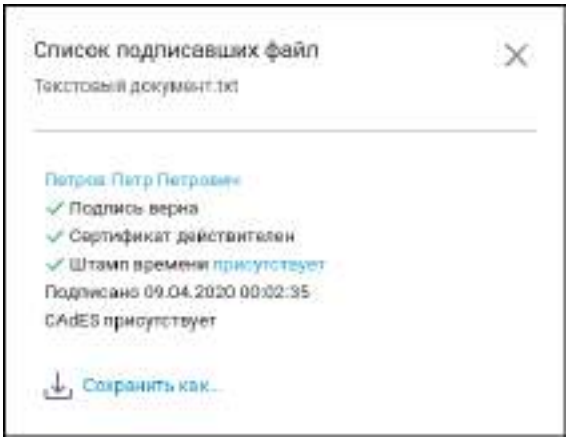

Рисунок 16. Результаты проверки подписи

6

Возможные неполадки и способы их устранения

Требуемый сертификат не отображается в списке сертификатов для подписи

При заверении файлов электронной подписью с помощью программы File Unit в окне **Выбор сертификата** нужный сертификат может не отображаться.

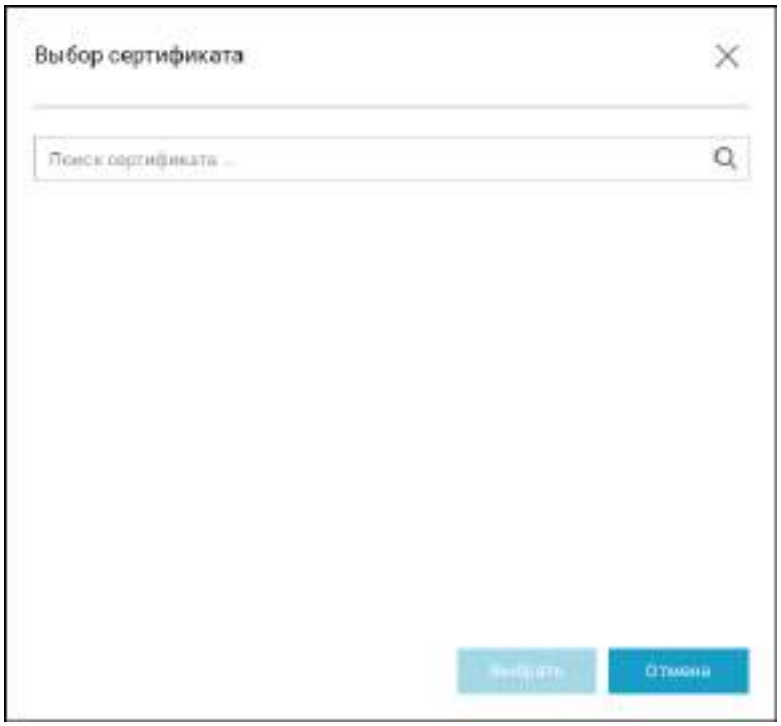

Рисунок 17. Сертификат не отображается в списке сертификатов для подписи

В этом случае нужно проверить, что для сертификата соблюдаются требования, перечисленные в разделе Требования к сертификатам для заверения электронной подписью и шифрования (на стр. 13).

Не отображаются значки компонентов в области уведомлений

Если вы используете ОС Ubuntu, и при запуске программ Web Unit и TLS значки этих программ не отображаются в области уведомлений, убедитесь, что у вас установлена оболочка для среды рабочего стола GNOME Classic (см. Системные требования на стр. 8).

При выборе зашифрованного файла недоступна операция расшифрования

При выборе зашифрованного файла кнопка **Расшифровать** может не отображаться.

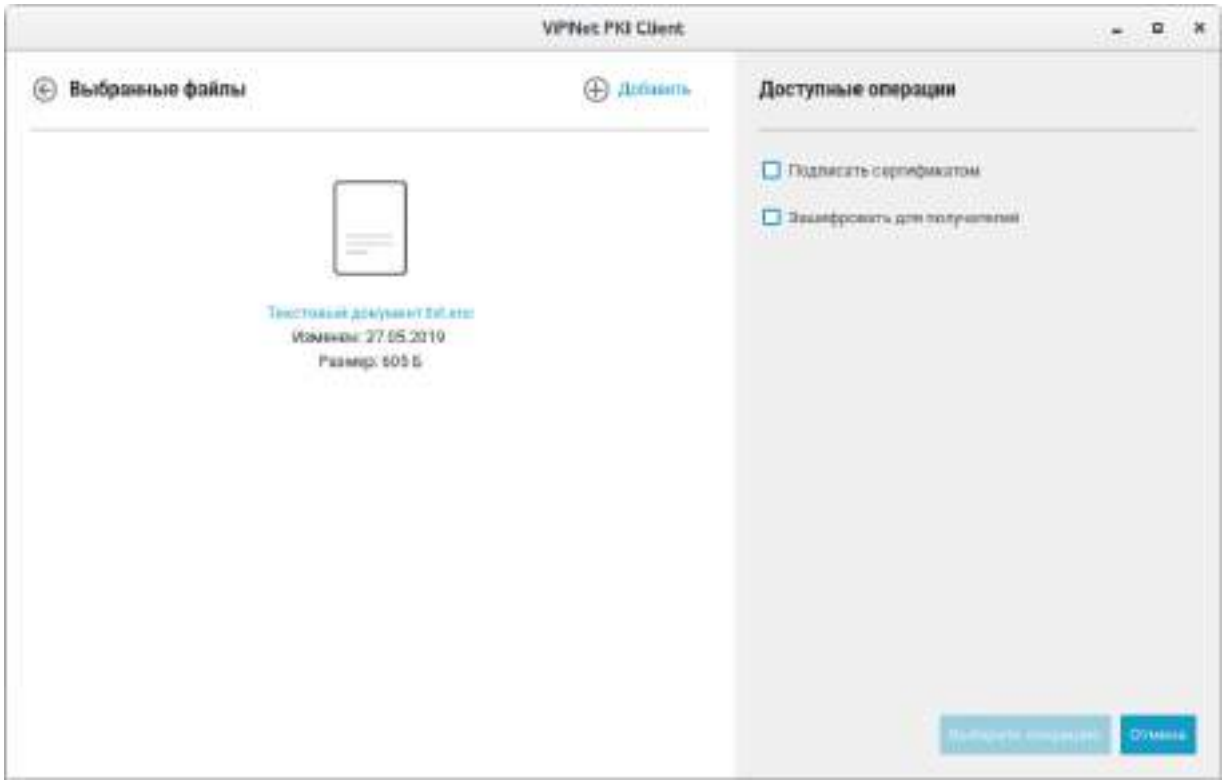

Рисунок 18. Окно выбора операции

Это означает, что в хранилище не найден подходящий для расшифрования сертификат, соответствующий требованиям, приведенным в разделе Требования к сертификатам для заверения электронной подписью и шифрования (на стр. 13).

Глоссарий

TSP-сервер (служба штампов времени)

Доверенный субъект инфраструктуры открытых ключей, обладающий точным и надежным источником времени и оказывающий услуги по созданию штампов времени.

ViPNet CSP Linux

Программа ViPNet CSP Linux представляет собой криптопровайдер и позволяет организовать выполнение криптографических операций на компьютерах, работающих под управлением операционных систем семейства Linux. Поддерживает алгоритмы электронной подписи и шифрования ГОСТ.

XMLDSig

Формат подписи, позволяющий подписывать не только весь XML-документ, но и его часть, причем разные части XML-документа могут быть подписаны разными пользователями.

Асимметричное подписание

Система подписания, при которой алгоритмы используют два математически связанных ключа. Закрытый ключ используется для подписи файла, а с помощью открытого ключа и сертификата пользователя подпись подтверждается.

Асимметричное шифрование

Система шифрования, при которой алгоритмы используют два математически связанных ключа. Открытый ключ используется для зашифрования и передается по незащищенному каналу. Закрытый ключ служит для расшифрования.

Ключ проверки электронной подписи

В соответствии с федеральным законом N 63-ФЗ «Об электронной подписи» от 6 апреля 2011 г. ключом проверки электронной подписи называется открытый ключ, который является не секретной частью пары асимметричных ключей и представляет собой уникальную последовательность символов, однозначно связанную с закрытым ключом и предназначенную для проверки подлинности электронной подписи.

Ключ электронной подписи

В соответствии с федеральным законом N 63-ФЗ «Об электронной подписи» от 6 апреля 2011 г. ключом электронной подписи называется закрытый ключ, который является секретной частью пары асимметричных ключей и представляет собой уникальную последовательность символов, предназначенную для создания электронной подписи.

Контейнер ключей

Файл или устройство, в котором хранятся ключ электронной подписи и соответствующий ему сертификат ключа проверки электронной подписи.

Открепленная подпись

Тип электронной подписи, при использовании которой электронная подпись и служебная информация помещаются в файл с расширением `*.sig` отдельно от исходного файла.

Например, при подписании `file.txt` открепленная электронная подпись помещается в контейнер `file.txt.sig`. Далее для проверки электронной подписи требуется не только данный контейнер, но и исходный файл, который в контейнер `file.txt.sig` не входит.

Прикрепленная подпись

Тип электронной подписи, при использовании которой исходный файл, электронная подпись и служебная информация помещаются совместно в один контейнер с расширением `*.sig`.

Например, файл `file.txt` заверяется прикрепленной электронной подписью и помещается в контейнер `file.txt.sig`. Далее для проверки электронной подписи требуется только данный контейнер, который содержит и электронную подпись, и исходный файл.

Сертификат издателя

Сертификат удостоверяющего центра, которым заверяются издаваемые сертификаты.

Сертификат ключа проверки электронной подписи

Электронный документ или документ на бумажном носителе, выданный удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающий принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.

Список аннулированных сертификатов (CRL)

Список сертификатов, которые до истечения срока их действия были аннулированы или приостановлены администратором Удостоверяющего центра и потому недействительны на момент, указанный в данном списке аннулированных сертификатов.

Удостоверяющий центр

Организация, осуществляющая выпуск сертификатов ключей проверки электронной подписи, а также сертификатов другого назначения.

Файл *.enc

Файл с расширением `*.enc`, который содержит в себе файл, зашифрованный с использованием ключа проверки электронной подписи получателя или нескольких получателей.

Файл *.sig

Файл с расширением `*.sig`, который содержит в себе электронную подпись, служебную информацию, сертификат ключа проверки электронной подписи, с помощью которого была сформирована данная электронная подпись, а также исходный файл (в случае использования прикрепленной подписи).

Цепочка сертификации

Упорядоченная последовательность сертификатов, соответствующая иерархии издателей этих сертификатов. Сертификат считается действительным, если цепочка сертификации полна (то есть завершается корневым сертификатом) и все входящие в нее сертификаты также действительны.

Штамп времени

Реквизит электронного документа, которым служба штампов времени удостоверяет, что в указанный момент времени ей было предоставлено значение хэш-функции данного документа. Штамп времени подтверждает точное время создания документа. Также может подтверждать время получения или отправления документа.

В штампе времени указывается следующее: значение хэш-функции документа, на который выдан штамп; идентификатор политики (OID), в соответствии с которой был выдан штамп; время выдачи штампа; точность времени и другие параметры.

Электронная подпись

Информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.